

Abstract

When a common key is updated to a new common key, it is possible to prevent the generation of a period during which not all the general communication apparatuses are enabled to make mutual communications using encrypted data while at the same time reducing the memory consumption of the general communication apparatus. A common key control apparatus 11 transmits a first status transition request R1 to all the general communication apparatuses when all the general communication apparatuses 12 made a transition to a distribution completed status, and transmits a second status transition request R2 to all the general communication apparatuses when all the general communication apparatuses 12 made a transition to an in-transit status. The general communication apparatus 12 makes a transition from the update completed status to the distribution completed status upon receipt of a new common key from the common key control apparatus 11, while it makes a transition from the distribution completed status to the in-transit status upon receipt of the first status transition request and it restores the state to the update completed status from the in-transit status upon receipt of the second status transition request.